BAB II

ANALISIS DAN PERANCANGAN

2.1 Analisis

2.1.1 *IPFire*

IPFIRE adalah *system* operasi yang digunakan sebagai *firewall, router, proxy server,* dan lain-lain yang berguna untuk mengamankan system jaringan komputer. *IPFIRE* didistribusikan dibawah *licensy GPL (General Public License) . IPFIRE* sendiri merupakan pengembangan dari *IPCOP* dan *Smoothwall* yang kemudian dikembangkan sendiri secara mandiri oleh *team* pengembang *IPFIRE*. Dalam mengembangkan proyek ini *team* pengembang *IPFIRE* menitik beratkan pada kemudahan instalasi, kemudahan konfigurasi karena *IPFIRE* dapat dikonfigurasi melalui *WEB interface* dan level keamanan, *team* pengembang *IPFIRE* juga benar-benar memperhatikan masalah keamanan jaringan komputer secara dinamis dan berkala agar tetap aman.

Dengan demikian *IPFIRE* sangat cocok digunakan untuk *network administrator* pemula maupun *profesional. IPFIRE* memiliki beberapa *fitur* penggunaan dalam system jaringan selain itu *IPFIRE* juga memiliki dukungan *add-on* yang membuat *IPFIRE* menjadi *firewall* yang handal dan aman. beberapa *fitur* yang dimiliki *IPFIRE* antara lain: Jika difungsikan sebagai *firewall*, *fokus* utama *IPFIRE* memang digunakan sebagai *firewall*,

ini berfungsi untuk mengatur kebijakan dalam autentikasi terhadap *system* jaringan. Layanan yang dapat djalankan antara lain:

- ✓ *inspeksi* berdasarkan arsitektur penyaringan jaringan *linux*.
- ✓ *Sistem* deteksi intruksi dengan *add-on Guardian* sebagai perpanjangan (*sistem IPS*).
- ✓ *filter* untuk tidak *valid* / paket.
- ✓ segmen jaringan yang terpisah untuk *server (DMZ)* dan nirkabel dengan kebijakan.
- ✓ perlindungan serangan *Dos* aplikasi *proxy* untuk *HTTP* dan *FTP* (dengan kontrol akses dan konten *filtering*) dan *DNS* masuk dan keluar packet *filtering* kualitas Layanan dan lalu lintas.

1. *IPFIRE* memiliki fungsi-fungsi penting dalam jaringan yaitu:

- ✓ *DHCP server*
- ✓ *Dynamic DNS service*
- ✓ *NTP server*
- ✓ *DNS proxy*

2. *http proxy*, Layanan *web proxy* memungkinkan untuk menyaring dan log aktivitas *user* dan mampu memblokir konten berbahaya. Seperti:

- ✓ *caching konten web.*
- ✓ Berdasarkan waktu penghentian akses untuk pengguna individu atau kelompok seluruh.
- ✓ manajemen yang disederhanakan untuk kelas atau ruang konferensi.
- ✓ Antivirus jadi penyimpanan *update* untuk *Microsoft Windows, Symantec Antivirus, Adobe produk, Avira Antivirus dan Avast Antivirus*.
- ✓ Otentikasi ke *LDAP*, identik, jari-jari atau *Windows server* atau *database* pengguna lokal.
- ✓ batasan transfer (kecepatan / atau volume lalu lintas).
- ✓ konten penyaringan berdasarkan daftar pemblokiran dan

  didefinisikan secara manual daftar untuk memblokir konten berbahaya.

3. *Virtual Private Networking, Virtual private network (VPN)* yang aman digunakan untuk berkomunikasi dengan pelanggan . Untuk maksimum interoperabilitas.
4. Jenis koneksi yang di dukung, *IPFire* dapat mengakses *internet* dengan banyak jenis koneksi yang umum.

- ✓ Penyambungan otomatis kembali setelah pemutusan oleh *Server*.

5. Konfigurasi *IPFIRE* dapat menggunakan *web interface* ataupun akses *ssh*.

6. *Monitoring,Administrator* jaringan dapat memonitor jaringan dengan mudah karena *IPFIRE* memiliki fungsi sebagai berikut :

   - ✓ Pemantauan grafis dari sistem dengan antarmuka *web*.
   - ✓ File log dapat diakses dengan ringkasan otomatis peristiwa penting.
   - ✓ Fungsi *ekspor file log(*individual atau sebagai *full backup)*

2.2 Peralatan yang diperlukan

2.2.1 *Router Mikrotik*

MikroTik adalah suatu *RouterOS (Router Operating System)* yaitu sistem operasi atau *software* yang dapat digunakan menjadi komputer *router network* yang handal dengan berbagai fitur yang dibuat untuk mengatur *ip network* dan jaringan *wireless*.

router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau *Internet* menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing. Router* berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya

2.2.2 *Hub/Switch*

Hub adalah sebuah perangkat jaringan komputer yang berfungsi untuk menghubungkan peralatan-peralatan dengan *ethernet 10BaseT* atau serat optik sehingga menjadikannya dalam satu segmen jaringan.

Switch adalah perangkat/komponen jaringan yang berperan sebagai jembatan untuk perangkat-perangkat jaringan sehingga masing-masing perangkat dapat terhubung satu dengan yang lain (menghubungkan komputer satu dengan yang lainnya). *Switch* memiliki sejumlah *port ethernet* untuk menghubungkan dirinya dengan perangkat-perangkat lain di jaringan.

Switch terbagi dalam 2 tipe utama: *switch layer-2* dan *layer-3. Switch layer-2* beroperasi pada layer *data-link model OSI* dan berdasarkan *teknologi bridging* (melakukan fungsi sebagai *bridge* antara *segmen-segmen* jaringan *LAN*, karena mereka meneruskan *frame Ethernet* berdasarkan alamat tujuannya tanpa mengetahui *protokol* jaringan apa yang digunakan). *Switch* tipe ini membangun koneksi logika antar *port* berdasarkan pada alamat *MAC* (alamat fisik).

2.2.3 *Cabling*

Kabel *UTP* atau kepanjangannya *Unshielded twisted-pair*. Kabel *UTP* adalah jenis kabel yang terbuat dari bahan penghantar tembaga, memiliki isolasi dari plastik dan terbungkus oleh bahan isolasi yang mampu melindungi dari api dan kerusakan fisik. Fungsi kabel *UTP*

digunakan sebagai kabel jaringan *LAN (Local Area Network)* pada sistem jaringan komputer, dan biasanya kabel *UTP* mempunyai impedansi kurang lebih 100 ohm. Kabel yang digunakan adalah *Cross* dan *Straight*. Kabel *Cross* Digunakan untuk menghubungkan perangkat jenis yang sama. Dan Kabel *Straight* Dapat digunakan untuk menghubungkan antar berbagai jenis perangkat yang berbeda.

2.2.4 *Client Server*

Client merupakan sembarang sistem atau proses yang melakukan suatu permintaan data atau layanan ke *server* sedangkan *server* adalah, sistem atau proses yang menyediakan data atau layanan yang diminta oleh *client. Client-Server* adalah pembagian kerja antara *server* dan *client* yang mengakses *server* dalam suatu jaringan. Jadi arsitektur *client - server* adalah desain sebuah aplikasi terdiri dari *client* dan *server* yang saling berkomunikasi ketika mengakses *server* dalam suatu jaringan.

2.2.5 *Putty*

Putty adalah *software remote console*/ terminal yang digunakan untuk *meremote* komputer dengan terhubungnya menggunakan *port ssh* atau sebagainya. Biasanya yang menggunakan *software Putty* adalah seorang administrator dan seorang *Hacker. Putty* juga bisa digunakan untuk menjalankan *PsyBNC, telnet* dan lain-lain.

2.2.6 *TEAMSPEAK*

2.1 *TeammSpeak 2 Client*

Gambar 2.1 Teamspeak.

TeamSpeak adalah sebuah perangkat lunak yang memungkinkan orang untuk saling berbicara satu sama lain melalui *internet. TeamSpeak* terdiri dari dua bagian , yaitu *server* dan *client. Server TeamSpeak* bertindak sebagai *host* yang akan menampung koneksi *client* darimanapun untuk bertemu dan berbicara dengan kapasitas sampai ribuan *client*.

Kelebihan *teamspeak* dapat *ber-chatting* di *internet* dengan dapat mendengarkan suara dari lawan *chatting* kita

- lebih *fleksibel* dan cepat
- *TS (TeamSpeak2)* juga memiliki 2 tipe *bit...*

  yaitu *32-bit* dan *64-bit* untuk *Windows*.

TeamSpeak banyak digunakan dalam *game online*, karena program ini sangat ringan dalam hal penggunaan *resource* dan *bandwitdh* komputer sehingga dapat dijalankan

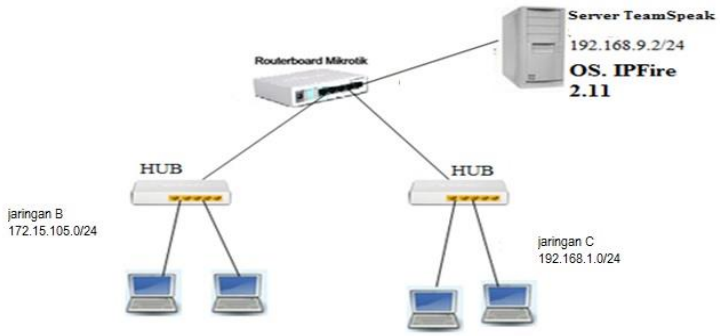
bersamaan dengan aplikasi lain, khususnya *game online*. Selain itu juga digunakan untuk memfasilitasi komunikasi antar kantor , antara rekan-rekan kerja, atau sekadar untuk komunikasi pribadi dengan teman dan keluarga. Bahkan saat ini *TeamSpeak* telah digunakan untuk sarana siaran radio nasional dan local.

TeamSpeak ini tidak berbayar. untuk non komersial dan biaya yang rendah dan lisensi yang mudah untuk penggunaan komersial.

2.2 *TeamSpeak2 Server*

Server TeamSpeak bertindak sebagai *host* yang akan menampung koneksi *client* dari manapun untuk bertemu dan berbicara dengan kapasitas sampai ribuan *client*. Dan *TeamSpeak server* berperan penting untuk mengatur semua *fitur – fitur* yang ada pada *TeamSpeak2 Client*

2.3 Rancangan Jaringan



Gambar 2.2 rancangan jaringan

Dari Gambar 2.2 Rancangan jaringan, komputer Server menggunakan *OS Ipfire* 2.11, yang nantinya akan diinstal *"add ons" Server TeamSpeak*, dan dapat diketahui juga, bahwa *server* yang terhubung dengan *Router* menggunakan jaringan *Green* mempunyai alamat *IP address* 192.168.9.2/24, pada jaringan A yang terhubung pada *Router* mempunyai alamat *IP address* 172.15.105.0/24, sedangakan pada jaringan B yang terhubung dengan *Router* mempunyai alamat *IP address* 192.168.1.0/24.

IP address server digunakan juga sebagai *IP Server TeamSpeak*, yang nantinya akan diakses oleh *TeamSpeak Client,* sehingga *Client* dapat berkomunikasi antara *Client* yang satu, dengan yang lainnya.

2.4 Data *Ip Address* dan *Subnetmask*

✓ ***Datagram Ethernet***

Sebuah paket data pada *Ethernet link* disebut *frame Ethernet*. Sebuah *frame* diawali dengan bingkai pembatas. Setiap *frame Ethernet* berlanjut dengan *header Ethernet* yang menampilkan tujuan dan sumber alamat *MAC*. Bagian tengah bingkai adalah data *payload* termasuk *header* untuk *protocol* lain (misalnya *Internet Protocol*) dilakukan dalam bingkai. Bingkai berakhir dengan *32-bit* cek *redundansi siklik* yang digunakan untuk mendeteksi adanya melebihkan atau mengurangi data dalam transit.

✓ **Struktur *Ethernet***

Sebuah paket data pada rangkaian disebut bingkai dan terdiri dari data *biner*. Data *Ethernet ditransmisikan oktet* paling *signifikan* pertama. Dalam setiap *oktet* bagaimanapun, *bit* yang paling *signifikan ditransmisikan* pertama. Tabel di bawah menunjukkan kerangka lengkap *Ethernet*, seperti yang di kirim, untuk ukuran *playload* hingga *MTU* 1500.

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
		← 64–1518 octets (68-1522 octets for 802.1Q tagged frames) →						
← 84–1538 octets (88-1542 octets for 802.1Q tagged frames) →								

Tabel 2.1 struktur frame Ethernet

- ✓ ***User Datagram Protokol (UDP)***

UDP, singkatan dari *User Datagram Protokol* adalah salah satu *protocol* lapisan *transport TCP/IP* yang mendukung komunikasi yang tidak handal *(unreriabel)*, tanpa *koneksi (connectionless*) antara *host-host* dalam jaringan *Transmission Control Protokol (TCP)* adalah suatu *protocol* yang berada di lapisan *transport* yang berorientasi sambungan *(connectionoriented)* dan dapat diandalkan *(reliable)*

- ✓ ***Transmission Control Protokol (TCP)***

Transmission Control Protokol (TCP) adalah suatu *protocol* yang berada di lapisan *transport* yang berorientasi sambungan. *(connection-oriented)* dan dapat diandalkan *(reliable).*

- ✓ ***SUBNET MASK* dan *Adress***

Subnet mask adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada angka *biner* 32 *bit* yang digunakan untuk membedakan *network ID* dengan *host ID,* menunjukkan letak suatu *host,* apakah berada di jaringan lokal atau jaringan luar.

IP adalah perpanjangan dari *Internet Protocol*. Biasanya, kalau disebutkan nama *IP* maka sebenarnya yang dimaksudkan adalah *IP Address* atau Alamat *IP*.

Pembagian kelas *IP*

10.100.1.1/8 255.0.0.0 kelas A

172.16.2.1 2/1655.255.0.0 kelas B

192.168.1.10/24 255.255.255.0 kelas C

Contoh:

192.168.1.20/24

Berapa maksimal Host/IP yang bisa dipakai?

24 = 24 + 0

0 0 0 0 0 0 0 0 (jumlah 0 adalah 8, maka n=8)

128 64 32 16 8 4 2 1

256 (28)

maka >> 256-2= 254 host

Kelas alamat	Subnet mask (biner)	Subnet mask (desimal)	Prefix Length
Kelas A	11111111.00000000.00000000.00000000	255.0.0.0	/8
Kelas B	11111111.11111111.00000000.00000000	255.255.0.0	/16
Kelas C	11111111.11111111.11111111.00000000	255.255.255.0	/24

Tabel 2.1Kelas alamat A,B, dan C

Sebagai contoh, *network identifier* kelas B dari 138.96.0.0 yang memiliki *subnet mask* 255.255.0.0 dapat direpresentasikan di dalam *notasi prefix length* sebagai 138.96.0.0/16.

Karena semua *host* yang berada di dalam jaringan yang sama menggunakan *network identifier* yang sama, maka semua *host* yang berada di dalam jaringan yang sama harus menggunakan *network*

identifier yang sama yang didefinisikan oleh *subnet mask* yang sama pula. Sebagai contoh, notasi 138.23.0.0/16 tidaklah sama dengan notasi 138.23.0.0/24, dan kedua jaringan tersebut tidak berada di dalam ruang alamat yang sama. *Network identifier* 138.23.0.0/16 memiliki *range* alamat *IP* yang *valid* mulai dari 138.23.0.1 hingga 138.23.255.254; sedangkan *network identifier* 138.23.0.0/24 hanya memiliki *range* alamat *IP* yang *valid* mulai dari 138.23.0.1 hingga 138.23.0.254.

- ✓ **Menentukan alamat *Network Identifier***

Untuk menentukan *network identifier* dari sebuah alamat IP dengan menggunakan sebuah *subnet mask* yaitu dengan menggunakan operasi logika bit-bit, nilai 1 akan didapat jika kedua bit yang diperbandingkan bernilai 1, dan nilai 0 jika ada salah satu di antara nilai yang diperbandingkan bernilai 0.

Cara ini akan melakukan sebuah operasi logika *AND comparison* dengan menggunakan 32-bit alamat IP dan dengan 32-*bit subnet mask*. Hasil dari operasi *bit* alamat *IP* dengan *subnet mask* itulah yang disebut dengan *network identifier*.

Contoh:

Alamat IP 10000011 01101011 10100100 00011010 (131.107.164.026)

Subnet Mask 11111111 11111111 11110000 00000000 (255.255.240.000)

Network ID 10000011 01101011 10100000 00000000 (131.107.160.000

- ✓ ***Subnetting* alamat *IP* kelas B**

Tabel berikut berisi *subnetting* yang dapat dilakukan pada alamat *IP* dengan *network identifier* kelas B

Jumlah subnet/ segmen jaringan	Jumlah subnet bit	Subnet mask (notasi desimal bertitik/ notasi panjang prefiks)	Jumlah host tiap subnet
1-2	1	255.255.128.0 atau /17	32766
3-4	2	255.255.192.0 atau /18	16382
5-8	3	255.255.224.0 atau /19	8190
9-16	4	255.255.240.0 atau /20	4094
17-32	5	255.255.248.0 atau /21	2046
33-64	6	255.255.252.0 atau /22	1022
65-128	7	255.255.254.0 atau /23	510
129-256	8	255.255.255.0 atau /24	254
257-512	9	255.255.255.128 atau /25	126
513-1024	10	255.255.255.192 atau /26	62
1025-2048	11	255.255.255.224 atau /27	30
2049-4096	12	255.255.255.240 atau /28	14
4097-8192	13	255.255.255.248 atau /29	6
8193-16384	14	255.255.255.252 atau /30	2

***Tabel 2.2 sabnet** ip kelas B*

- ✓ **Subnetting Alamat IP kelas C**

Tabel berikut berisi subnetting yang dapat dilakukan pada alamat IP dengan *network identifier* kelas C.

Jumlah subnet (segmen jaringan)	Jumlah subnet bit	Subnet mas1265132185131813k (notasi desimal bertitik/ notasi panjang prefiks)	Jumlah host tiap subnet
0-1	0	255.255.255.0 atau /24	254
1-2	1	255.255.255.128 atau /25	126
3-4	2	255.255.255.192 atau /26	62
5-8	3	255.255.255.224 atau /27	30
9-16	4	255.255.255.240 atau /28	14
17-32	5	255.255.255.248 atau /29	6

tabel 2.3 subnet IP kelas C